Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (Original) A networked system for accessing information, comprising:

a first network station, representing a first network entity, configured to control access to information stored on a network for a third network entity, and to encrypt a first component message with a first crypto-key associated with the first network entity;

a second network station, representing a second network entity, configured to control access to the network by the third network entity, to encrypt a second component message with a second crypto-key, to combine the encrypted first and the encrypted second component messages, and to transmit the combined messages over the network; and

a third network station, representing the third network entity, configured to receive the transmitted combined messages and to further transmit the received combined messages over the network in order to obtain access to the stored information;

wherein the first network station is further configured to receive the further transmitted combined messages, to decrypt the encrypted first and the encrypted second component messages in the received further transmitted combined messages, and to control access by the third network station to the stored information based on the decrypted first and second component messages.

Claim 2 (Original) A networked system according to claim 1, wherein:

the first crypto-key is a symmetric crypto-key; and

the second crypto-key is a non-symmetric crypto-key.

Claim 3 (Original) A networked system according to claim 2, wherein:

the symmetric crypto-key is known only to the first network entity.

Claim 4 (Original) A networked system according to claim 2, wherein;

the non-symmetric crypto-key is a private crypto-key of a joint private-public crypto-key pair associated with the second network entity.

Claim 5 (Original) A networked system according to claim 1, wherein:

the first crypto-key is a first non-symmetric crypto-key; and

the second crypto-key is a second non-symmetric crypto-key, different than the first non-symmetric crypto-key.

Claim 6 (Original) A networked system according to claim 5, wherein:

the first non-symmetric crypto-key is a public crypto-key of a joint private-public crypto-key pair associated with the first network entity; and

the second non-symmetric crypto-key is a private crypto-key of a joint private-public crypto-key pair associated with the second network entity.

Claim 7 (Original) A networked system according to claim 1, wherein;

the first component message includes identity information associated with the third network entity, and integrity information which corresponds to the identity information; and

the second component message includes voucher information which indicates that the second network entity has authenticated the third network entity.

Claim 8 (Original) A networked system according to claim 1, further comprising:

a fourth network station, representing a fourth network entity, configured to encrypt a third component message with a third crypto-key, to initially combine the encrypted first and the encrypted third component messages, and to transmit the initially combined messages over the network;

wherein the second network station is further configured to receive the transmitted initially combined messages, to combine the encrypted first and the encrypted third component messages in the received initially combined messages with the encrypted second component message to create the combined messages;

wherein the first network station is further configured to decrypt the encrypted third component message in the received further transmitted combined messages, and to control access by the third network station to the stored information based also on the decrypted third component message.

Claim 9 (Original) A networked system according to claim 8, wherein:

the first component message includes identity information associated with the third network entity, and integrity information which corresponds to the identity information;

the second component message includes voucher information which indicates that the second network entity has authenticated the third network entity; and

the third component message includes relationship information which indicates that the identity and the integrity information was received by the fourth network entity from the first network entity and transmitted by the fourth network entity to the second network entity.

Claim 10 (Original) A networked system according to claim 8, wherein:

the first crypto-key is a symmetric crypto-key;

the second crypto-key is a non-symmetric crypto-key; and

the third crypto-key is a non-symmetric crypto-key.

Claim 11 (Original) A networked system according to claim 1, wherein:

the second component message further includes a timestamp corresponding to a time at which the combined messages are transmitted by the second network station.

Claim 12 (Original) A networked system according to claim 1, wherein:

the first network station is further configured to combine the encrypted first component message with a network address for the stored information;

the second network station is further configured to combine the combined encrypted first component message and the network address with the encrypted second component message to create the combined messages; and

the first network station is further configured to control access by the third network station to the stored information based on the network address and the decrypted first and second component messages.

Claim 13 (Original) A networked system according to claim 1, wherein:

the second network station transmits the combined message in response to a received request;

the first network station encrypts the first component message prior to receipt of the request by the second network station; and

the second network station encrypts the second component message and combines the encrypted first and the encrypted second component messages after receipt of the request by the second network station.

Claim 14 (Original) A method of creating an electronic message for transmission over a network, comprising the steps of:

encrypting a first component with a first crypto-key, associated with a first network entity, such that the encrypted first component can be decrypted by only the first network entity;

encrypting a second component with a second crypto-key, associated with a second network entity, such that the encrypted second component can be decrypted by the first network station; and

transmitting the encrypted first component and the encrypted second component as a combined message.

Claim 15 (Original) A method according to claim 14, wherein:

the first crypto-key is a symmetric crypto-key; and

the second crypto-key is a non-symmetric crypto-key.

Claim 16 (Original) A method according to claim 15, wherein;

the symmetric crypto-key is known only to the first network entity; and

the non-symmetric crypto-key is known only to the second network entity.

Claim 17 (Original) A method according to claim 15, wherein;

the non-symmetric crypto-key is a private crypto-key of a joint private-public crypto-key pair associated with the second network entity.

Claim 18 (Original) A method according to claim 14, wherein:

the first crypto-key is a first non-symmetric crypto-key; and

the second crypto-key is a second non-symmetric crypto-key.

Claim 19 (Original) A method according to claim 18, wherein:

the first non-symmetric crypto-key is a public crypto-key of a joint private-public crypto-key pair associated with the first network entity; and

the second non-symmetric crypto-key is a private crypto-key of a joint private-public crypto-key pair associated with the second network entity.

Claim 20 (Original) A method according to claim 14, further comprising the steps of:

encrypting a third component with a third crypto-key, associated with a third network entity, such that the encrypted third component can be decrypted by the first network entity; and

transmitting the encrypted third component with the encrypted first and the encrypted second components as the combined message.

Claim 21 (Original) A method according to claim 20, wherein:

the first crypto-key is a symmetric crypto-key;

the second crypto-key is a first non-symmetric crypto-key; and

the third crypto-key is a second non-symmetric crypto-key.

Claim 22 (Original) A method according to claim 20, wherein:

the first component includes identity information associated with a fourth network entity and integrity information corresponding to the identity information;

the second component includes relationship information which indicates that the identity and the integrity information were received by the second network entity from the first network entity and transmitted by the second network entity to the third network entity; and

the third component includes voucher information which indicates that the third network entity authenticated the fourth network entity.

Claim 23 (Original) A method according to claim 20, wherein:

the third component further includes a timestamp corresponding to a time at which the combined message is transmitted to the fourth network entity.

Claim 24 (Original) A method according to claim 20, further comprising the step of: transmitting the encrypted first, the encrypted second and the encrypted third components with a network address as the combined message.

Claim 25 (Original) A method according to claim 14, wherein:

the combined message is transmitted responsive to a received request;

the first component is encrypted prior to receipt of the request; and

the second component is encrypted after receipt of the request.

Claim 26 (Currently Amended) ~~An~~A method for generating a multi-component electronic message, comprising:

storing (i) a first component created by a first network entity and encrypted with a first crypto-key, associated with the first network entity, such that the encrypted first component can be decrypted by only the first entity~~;~~ and (ii) a second component created by a second network entity, and encrypted with a second crypto-key, such that the encrypted second component can be decrypted by the first network entity; and combining the stored first component with the stored second component to generate a multi-component message.

Claim 27 (Currently Amended) ~~An electronic message~~The method according to claim 26, wherein:

the first crypto-key is a symmetric crypto-key known only to the first network entity; and

the second crypto-key is a non-symmetric crypto-key.

Claim 28 (Currently Amended) ~~An electronic message~~The method according to claim 27, wherein;

the non-symmetric crypto-key is a private crypto-key of a joint private-public crypto-key pair associated with the second network entity.

Claim 29 (Currently Amended) ~~An electronic message~~The method according to claim 26, wherein:

the first crypto-key is a first non-symmetric crypto-key; and

the second crypto-key is a second non-symmetric crypto-key.

Claim 30 (Currently Amended) ~~An electronic message~~The method according to claim 29, wherein:

the first non-symmetric crypto-key is a public crypto-key of a joint private-public crypto-key pair associated with the first network entity; and

the second non-symmetric crypto-key is a private crypto-key of a joint private-public crypto-key pair associated with the second network entity.

Claim 31 (Currently Amended) ~~An electronic message~~The method according to claim 26, further comprising:

storing a third component created by a third network entity and encrypted with a third crypto-key, associated with the third network entity, such that the encrypted third component can be decrypted by the first network entity;

wherein the stored third component is combined with the stored first and stored second components to generate the multi-component message.

Claim 32 (Currently Amended) ~~An electronic message~~The method according to claim 31, wherein:

the first component includes identity information associated with a fourth network entity, and integrity information corresponding to the identity information;

the second component includes relationship information which indicates that the identity and the integrity information were received by the second network entity from the first network entity and transmitted by the second network entity to the third network entity; and

the third component includes ~~voucher~~ information which indicates that the third network entity has authenticated the fourth network entity.

Claim 33 (Original) An electronic message according to claim 32, wherein:

the integrity information includes a hash of the identity information.

Claim 34 (Currently Amended) ~~An electronic message~~The method according to claim 32, wherein:

the third component further includes a timestamp corresponding to a time at which the electronic message is transmitted by the third network entity to the fourth network entity.

Claim 35 (Currently Amended) ~~An electronic message~~The method according to claim 26, wherein:

the first component includes identity information associated with a third network entity;

the second component includes ~~voucher~~ information which indicates that the second network entity has authenticated the third network entity.

Claim 36 (Currently Amended) ~~An electronic message~~The method according to claim 35, wherein:

the second component further includes a timestamp corresponding to a time at which the electronic message is transmitted by the second network entity to the third network entity.

Claim 37 (Currently Amended) ~~An electronic message~~The method according to claim 26, wherein:

the first network entity controls access to information available on a network; and

the second entity controls access to other network entities.

Claim 38 (Currently Amended) ~~An electronic message~~The method according to claim 26, wherein the first component includes an identification of information stored on a network, and further comprising:

combining a network address at which the identified stored information can be accessed with the generated multi-component message.

Claims 39-49 (Cancelled)